Bank of Cyprus

TERMS OF REFERENCE OF THE GROUP BOARD RISK COMMITTEE

1. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Explanation
AC	Audit Committee
ADC	Acquisition Disposal Committee
Bank	Bank of Cyprus Holdings Public Limited Company (BOCH) and its subsidiary Bank of Cyprus PCL
Board	The Board of the Bank
CET1	Common Equity Tier 1
CMRC	Crisis Management and Response Committee
Chair	The Chair of the Committee
Committee	Group Risk Committee
C&E	Climate-related and Environmental
ExCo	Executive Committee
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
Group	Bank and all its subsidiaries
HRRC	Human Resources & Remuneration Committee
ICAAP	Internal Capital Adequacy Assessment Process
ICT	Information and Communication Technology
ILAAP	Internal Liquidity Adequacy Assessment Process
NCGC	Nomination and Corporate Governance Committee
RAF	Risk Appetite Framework
OSP	Outsourcing Service Providers
O-SII	Other Systemically Important Institutions
SRT	Significant Risk Transfer
Invitees	A person who is not a committee member but is formally invited to attend for a specific item(s) on the agenda.

2. AUTHORITY

2.1 The Committee is a statutory Committee of the Board of the Bank from which it obtains its authority and to which it regularly reports.

2.2 The Committee has been delegated authority by the Board in respect of the functions and powers in these Terms of Reference.

2.3 The Committee is concerned with the business of the Bank, its business units, and subsidiaries, and accordingly its authority extends to all relevant matters relating to the Group.

2.4 The Committee has authority to investigate any matters within the scope of its terms of reference calling on whatever resources (including external professional or legal services) and to obtain such information as it may require from any director, officer, or employee of the Group. It has access to adequate funding to enable it to discharge its duties.

2.5 The Chair is authorised in this respect to provide approval of expenditure up to a maximum of €20.000 and he/she is required to inform the Committee at the next meeting.

2.6 For other risk-related engagements the Chair of the Committee is authorised to provide preliminary approval up to €150.000 with the requirement that upon such approval all Committee members are notified (through an e-mail) and they provide their positive confirmation.

2.7 The Committee reviews annually the Terms of Reference and recommends necessary amendments to the Board.

2.8 Although the Board has delegated authority to the Committee (including such matters that may be considered and reviewed independently from the executive Directors), the Board as a whole retains ultimate responsibility for the proper and adequate risk management of the Group (including the assessment of applicable risks and setting the Group's risk appetite) and it should reach its own conclusions regarding the reports and recommendations it receives.

3. ROLE OF THE COMMITTEE

The main purpose of the Committee is to review, on behalf of the Board, the aggregate Risk Profile of the Group, including performance against Risk Appetite for all risk types and ensure both the Risk Profile and Risk Appetite remain appropriate. Specifically, it will:

3.1 Assist the Board in overseeing the implementation of the Group's risk strategy and the corresponding limits set.

3.2 Oversee the identification, assessment, control and monitoring of financial / economic risks and non-financial risks (including operational, technological, legal, reputational, compliance and ESG risks including C&E risks (C&E)), which the Group faces in cooperation with other responsible Board Committees.

3.3 Advise and support the Board regarding the monitoring of the Group's overall actual and future risk appetite and strategy to ensure that they are in line with the business strategy, objectives, corporate culture, and values of the Group.

3.4 Consider, challenge, and recommend to the Board for approval the Group's overall Risk Appetite.

3.5 Review the aggregated Risk Profile for the Group and performance against Risk Appetite and report its conclusions to the Board.

3.6 Identify the potential impact of emerging issues and themes that may affect the Risk Profile of the Group.

3.7 Ensure that the Group's overall Risk Profile and Risk Appetite remain appropriate given the evolving external environment, the Group's character, and the internal control environment.

3.8 Seek to identify and assess future potential risks which, by virtue of their uncertainty, of low probability and unfamiliarity may not have been factored adequately into review by other Board Committees.

3.9 Ensure effective and on-going monitoring and review of the Group's management or mitigation of risk, including the Group's control processes, training and culture, information and communication systems and processes for monitoring and reviewing their continuing effectiveness.

3.10 Oversee the implementation of the strategies for capital and liquidity management as well as for the overall risks of the Group to assess their adequacy against the approved risk

appetite and strategy and to evaluate the adequacy of the forecasts and the effectiveness of the strategies and policies regarding maintenance, on continuous basis, of sufficient amounts, types and distribution of internal capital and equity to cover the risks of the Bank.

3.11 Ensure the effective management of all risks associated with outsourcing.

3.12 Provide recommendations to the Board on necessary adjustments to the risk strategy resulting from, inter alia, changes in the business model of the Bank, market developments or recommendations made by the Risk Management Division.

3.13 The Risk Management Division reports to the Board through the Committee.

4. COMMITTEE COMPOSITION

4.1 The Committee comprises of at least three members. The Committee must consist entirely of independent non-executive Directors who possess individually and collectively adequate knowledge, skills, and expertise to fully understand and monitor the risk strategy and the risk appetite of the Group as well as its risk management and control practices.

4.2 The Committee is chaired by a non-executive independent member of the Board.

4.3 The Committee interacts with other committees appropriately. Such interaction takes the form of cross-participation so that the Chair or a member of the Committee could also be a member of another committee (e.g. the Chairs of the Committee and the AC can respectively be members of the AC and the Committee, however, any further cross-participation of other members should be avoided as this could be classed as overlap).

4.4 The Chair cannot be the Chair of the Board or the chairperson of any other statutory Committee of the Board.

4.5 The Board appoints the members of the Committee annually and on an ad hoc basis on the recommendation of the NCGC in consultation with the Chair of the Committee.

4.6 The maximum number of terms for which an individual may serve as Chairperson of the Committee respects the limit of the total term as a member of the Board that applies for the purposes of independence of members of the Board.

5. COMMITTEE MEETINGS

5.1 The Committee holds regular meetings, at least four (4) per year and additionally, ad hoc meetings whenever called by the Chair of the Committee. Every effort is exercised to hold at least one meeting a year with physical presence of all members.

5.2 As a general rule, notice of meetings together with the agenda and support material of the items to be discussed are forwarded to each member of the Committee or any other person required or invited to attend no later than five (5) working days before the date of the meeting.

5.3 The Company Secretary or his/her nominee record and maintain detailed minutes of the meetings of the Committee, including noting the names of those present and in attendance. Draft minutes must be finalised no later than fifteen (15) business days following the meeting, formally approved at the next meeting, and at the same time be submitted to the Board for noting.

5.4 The quorum for a meeting is two (2) members or 50% rounded up, whichever is the highest.

5.5 Questions arising at any meeting are decided by a majority of votes. In case of an equality of votes the Chair has a second or casting vote.

5.6 The Board's direction for minimum annual attendance requirements for Committees of the Board require Committee members to participate in at least 3/4 of all meetings (regular and extraordinary) and that any continuous absences not to exceed 2 in number.

5.7 No person other than a committee member is entitled to attend meetings of the Committee. Invitees are formally invited to committee meetings only for a specific item(s) on the agenda and leave the meeting immediately afterwards, without any participation in the discussion/decision-making process.

5.8 The Committee annually establishes a schedule of major topics to be discussed during the year.

5.9 Decisions beyond this Committee's authority and matters which any member of the Committee deems necessary for escalation will be escalated by the Chair to the Board as appropriate.

6. RESPONSIBILITIES

6.1 Risk Appetite and Strategy

Risk Appetite, Strategy and Profile

6.1.1 Review management proposals on the desired risk strategy of the Group, in each area of risk (e.g. market, liquidity, credit, equity, regulatory, information security, operational reputational, ESG, digital and capital resources, and ESG, including C&E risks), oversee its implementation, in order to assess its adequacy against the approved risk appetite and strategy and make appropriate recommendations to the Board.

6.1.2 Advise and support the Board on the Group's overall actual and future risk appetite and strategy, taking into account all types of risk, to ensure they are in line with the business strategy, objectives, corporate culture and values of the institution.

6.1.3 Report to the Board any current and emerging topics relating to ESG risks and matters, including C&E risks and matters that are expected to materially affect the business. Operations, performance, or public image of the Group or are otherwise pertinent to the Group and its stakeholders and if appropriate, detail actions taken in relation to the same.

6.1.4 Examine the adequacy and effectiveness of the contingency and insurance strategy of the Group and make appropriate recommendations to the Board.

6.1.5 Assist the Board in setting the Group's risk culture and its communication to management.

Risk strategy oversight

6.1.6 Submit to the Board proposals and recommendations for corrective action whenever weaknesses are identified in implementing the risk strategy resulting from, inter alia, changes in the business model of the institution, market developments or recommendations made by the Risk Management Division.

6.1.7 Regularly monitor and ensure compliance of the Group with the adopted risk strategy by reviewing exception reports prepared by the Risk Management Division and any other information the Committee considers necessary and make recommendations to and inform the Board on the significant risks to which the Bank is exposed.

6.1.8 Examine management reports concerning changes anticipated in the economic and business environment, or major internal changes and the extent to which they affect the Group's risk profile and appetite and make appropriate recommendations to the Board.

6.1.9 Determine the nature, the amount, the format, and the frequency of the information on risk that the Committee desires to receive on the risk position of the Group and, if appropriate of

each business unit in order to properly carry out its roles to review, monitor and provide assurance or recommendations to the Board in its areas of responsibility and when there are gaps, how they are to be addressed.

6.1.10 Assist the Board in overseeing the effective implementation of the risk strategy by senior management, including the development of mechanisms to ensure material exposures that are close to, or exceed approved risk limits are managed and where necessary, mitigated in an effective and timely manner and ensure the identification and escalation of breaches in risk limits and of material risk exposures in a timely manner.

6.1.11 Ensure that risk parameters and risk models developed and used to quantify risk exposures are subject to periodic independent validation.

6.1.12 Examine high-risk transactions and make recommendations to the Board.

6.1.13 Examine whether incentives provided by the remuneration system adequately take into consideration risk, capital, liquidity and the likelihood and timing of earnings without prejudice to the tasks of the HRRC.

Financial products Risks

6.1.14 Oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the Bank.

6.1.15 Assess the risks associated with offered financial products and services taking into account the alignment between the prices assigned to and the profits gained from those products and services. Where the prices do not properly reflect the risks in accordance with the business model and the risk strategy, the Committee presents a remedy plan to the Bank.

Control Functions / Audit Recommendations

6.1.16 Assess and monitor the independence, adequacy and effectiveness of the Risk Management Division and the Information Security function and advice the Board accordingly including on the adequacy and effectiveness of overall risk appetite and Information Security frameworks, which, inter alia, ensures the adequate protection of confidential and personal information of the Bank.

6.1.17 Assess the recommendations of internal or external auditors relevant to Risk Management or InfoSec matters and follow up on the appropriate implementation of measures taken.

Group Risk Oversight

6.1.18 The Committee is responsible for the oversight of the whole Group but may delegate tasks to subsidiary risk committees to avoid duplication.

6.1.19 The Committee reviews the composition, authorities, duties and responsibilities and effectiveness of other Risk Committees (where such Committees are appointed), that function within the Group and where necessary make recommendations to the respective subsidiary Board for rectification.

6.1.20 The Committee evaluates the Group's governance, risk and control framework and oversee its integration with the Bank's decision-making process, covering the whole spectrum of the Bank's activities and units as well as subsidiaries.

6.2 Risk Policies and Risk Management

Risk Policies

6.2.1 Determine the principles that should govern the management of risks, (including ESG and C&E risks) through the establishment of appropriate Risk Policies.

6.2.2 Review and recommend for approval all such risk policies.

6.2.3 Monitor and ensure compliance of the Group with risk management policies, and regulatory requirements and make appropriate recommendations to the Board.

Adequacy and Effectiveness Assessment

6.2.4 Jointly with AC review provisions proposals by management and other topics of common/shared responsibility and make appropriate recommendations to the Board in relation to the adequacy of these provisions and the methodology adopted.

6.2.5 Advice the Board, drawing on the work of the Audit Committee, the Risk Management Division, Information Security function and external auditors, on the adequacy and effectiveness of the Risk Management and Information Security Policies and Framework.

6.2.6 Advise the Board, drawing on the work of the Audit Committee, the Risk Management Division, Information Security function and external auditors, on the adequacy and robustness of information and communication systems to enable identification, measurement, assessment, and reporting of risk in a timely and accurate manner and ensure the adequate protection of the institution's confidential and proprietary information.

6.2.7 Advise the Board, drawing on the work of the AC, the CRO and external auditors, on the adequacy of capital resources in relation to the level of undertaken risks with respect to maintaining on an ongoing basis, amounts, types, and distribution of both the internal capital and own funds adequate to cover the risks to the institution.

6.2.8 *Carry out robust assessment of the Group's emerging and principal risks. Focus should be given to those risks that given the Group's current position, could threaten the Group's business model, future performance, solvency, or liquidity, irrespective of how they are classified or from where they arise.*

Internal Risk Reporting & Regulatory Reporting

6.2.9 Review and recommend to the Board for approval the Annual Risk Management Report and the Annual Information Security Risk Report.

6.2.10 Review, evaluate and make any relevant recommendations to the Board on the ICAAP report which aims to assess all important risks undertaken by the Group and determine capital requirements of the Group. Ensure that the Group's risk profile is in line with the risk appetite and capital planning approved by the Board.

6.2.11 Review, evaluate and make relevant recommendations to the Board on the ILAAP report which aims to assess all risk to the Group's liquidity and ensures that the Group's risk profile is in line with the Group's liquidity adequacy and its strategic plans.

Stress testing / O-SII buffer

6.2.12 Ensure that the O-SII buffer is maintained within the limits set by the Central Bank on an individual and consolidated basis, and which consists of and is supplementary to CET1 Capital.

6.2.13 Ensure that stress tests and related procedures are carried out as appropriate on all major risks, at least on an annual basis and where necessary, challenge the appropriateness of limits and adequacy of capital and budgets.

6.2.14 Review a number of possible scenarios, including stressed scenarios, to assess how the institution's risk profile would react to external and internal events.

Recovery Plan / SRT

6.2.15 Review and recommend for approval to the Board the Recovery Plan and any revisions thereof.

6.2.16 Oversee the SRT framework, monitor compliance with the SRT Policy, review SRT transactions and make recommendations to the Board for approval.

6.2.17 Assess stress situations escalated by the ExCo through the review and assessment of the recovery and early warning indicators and decide whether to escalate further to the Board with a recommendation to declare a 'Recovery Emergency Situation' and perform an assessment of the Recovery Options.

6.2.18 Recommend to the Board to assign responsibility to the CMRC for the implementation of the Recovery Plan.

AML

6.2.19 Jointly with the AC oversee information on regulatory compliance, to prevent and combat money laundering, including access to aggregate information.

ESG and C&E

6.2.20 Review and monitor key enterprise wide ESG including C&E metrics, targets, KPIs, KRIs and related goals and monitor the progress towards achieving targets and benchmarks.

6.2.21 Receive and review periodic reports from management on ESG and climate trends, issues, and risks, including developments in applicable regulations, as well as the corresponding mitigation initiatives and controls.

6.2.22 Review on an ongoing basis whether existing policies comprehensively cover C&E risks, including the credit policies for each sector and product.

Oversight of control functions

6.2.23 Review and approve the budgets of the Risk Management Division and Information Security function, ensuring that they are sufficiently flexible to adapt to variations in response to developments.

6.2.24 Evaluate the CRO and the CISO and recommend to the Board, as appropriate, their appointment, replacement, reassignment, or dismissal. Carry out their annual appraisals and submit them to the Board.

Outsourcing

6.2.25 Oversee the Outsourcing Framework and ensure effective managing of all risks associated with outsourcing.

6.2.26 Review any planned changes regarding OSPs and the potential impact of these changes on the critical or important functions.

6.2.27 Obtain a report summarising the risk analysis, including legal risk, compliance with regulatory requirements and the impact on service levels relevant to the above changes.

Risk Culture

6.2.28 Obtain adequate assurance that:

a. the Senior Executive Management fully comprehends and applies the acceptable risk-taking levels, as defined by the Board,
b. all employees comprehend and apply the risk taking and risk management policy and
c. excessive risk-taking is not encouraged.

6.3 Approval of Loans and Limits

6.3.1 The Committee will review and recommend to the Board for approval special or urgent cases of loans, write-offs, DFAS and other Credit Risk requests as these may be submitted by CC3 and/or ADC and as per delegated authorization levels by the Board and above authorities delegated to management.

6.3.2 Review and recommend to the Board for approval changes to market and other nonfinancial risk limits not delegated to the Management Committees.

6.4 Digital Operational Resilience

6.4.1 The Committee also advises the Board on how to:

(a) bear the ultimate responsibility for managing the Bank's ICT risk.

(b) ensure that there are policies in place that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality of data.

(c) set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions.

(d) bear the overall responsibility for setting and approving the digital operational resilience strategy including the determination of the appropriate risk tolerance level of ICT risk of the Bank.

(e) approve, oversee and periodically review the implementation of the Bank's ICT business continuity policy and ICT response and recovery plans, which may be adopted as a dedicated specific policy forming an integral part of the Bank's overall business continuity policy and response and recovery plan.

(f) approve and periodically review the Bank's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers.

(g) put in place, at corporate level, reporting channels enabling it to be duly informed of the following:

(i) arrangements concluded with ICT third-party service providers on the use of ICT services,

(ii) any relevant planned material changes regarding the ICT third-party service providers,

(iii) the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.

6.5 Data & Report Quality

6.5.1 Jointly with AC proposes to the Board the Group's desired level of compliance with BCBS 239 principles on "Effective Risk Data Aggregation and Risk reporting" and monitors the progress/status of compliance via the effective implementation of the Data Quality and Governance framework.

6.5.2 Jointly with the AC defines Group's risk tolerance thresholds on Data Quality KRIs integrated in the RAF of the Group.

6.5.3 Jointly with AC proposes to the Board the risk metrics and reports for each category in both baseline (normal times) and adverse (times of stress/crisis) scenarios, as well as corresponding data quality and frequency requirements.

6.6 Communication and Reporting

6.6.1 Ensure adequate coordination/communication exists between the Board and the management on risk management and information security issues.

6.6.2 Liaise with other Committees of the Board as appropriate, including with the HRRC in relation to the remuneration of persons within the Group's risk management and information security functions.

6.6.3 *The Risk Committee should meet periodically with the Audit and other risk-relevant Committees to ensure effective exchange of information and effective coverage of all risks, including emerging risks and any needed adjustments are made to the risk governance framework of the Group in the light of its business plans and the external environment.*

6.6.4 *Have access to all relevant information and data necessary to perform its role including information and data from relevant corporate and control functions, for instance legal, financial, human resources, risk, ICT, information security, audit, and compliance.*

6.6.5 *Ensure that submissions by the Risk Management Division, the Compliance Division, the Information Security Function, and everyone else are appropriately documented.*

6.6.6 Formulate the Annual Risk Committee Report included in the Annual Corporate Governance Report of the Group, which should include the following:

a) Confirmation that the Risk Committee has carried out a robust assessment of the principal risks and uncertainties facing the Group, including those that would threaten its business model, future performance, solvency, or liquidity.

b) An explanation of these risks and how the Group has managed and mitigated such risks during the period and what procedures are in place to identify and manage emerging risks.

c) An assessment of the adequacy and effectiveness of the Group's risk management and internal control systems during the previous year.

d) An assessment of the appropriateness of limits of risks and the adequacy of provisions and capital.

e) An indication of the Committee's membership, the number of its meetings and attendance over the year and its main activities.

6.6.7 Examine and approve the circumstances under which the Chair can engage in communication with the main shareholders through the Senior Independent Director or in collaboration with the Senior Independent Director.

6.6.8 Respond, through the Chair, to shareholder questions regarding Group risk management issues at the Annual General Meeting.

6.6.9 Report to the Board regularly on how the Committee discharges its responsibilities, on the nature and content of discussion at Committee meetings, its recommendations, and actions to take.

6.6.10 The CRO and the CISO will meet regularly with the Chair and will have the right and responsibility to elevate issues to the Chair where they consider it necessary in the furtherance of their responsibilities.

6.6.11 The Chair arranges to hold an annual conference call with all chairpersons of subsidiary Audit & Risk Committees and reports to the Board any concerns.

6.6.12 Annually obtain and review the report on risk committee performance of each major subsidiary and take appropriate action.

6.6.13 *Provide advice on the appointment of external consultants that the Board may decide to engage for advice or support.*

6.6.14 *Conduct a self-assessment and report to the Board the Risk Committee's conclusions and recommendations for improvements and changes*.

6.6.15 Ensure that the Committee's terms of reference are available on the Group's official website.